

EPIC's 20th
Washington, DC
June 2, 2014

Prepared Remarks

Marc Rotenberg

WELCOME

Thank you, Bruce.

Bruce was a co-plaintiff in EPIC's successful challenge to the TSA's backscatter X-ray program. It took almost 5 years, and there were three mandamus petitions. But the government no longer gets to irradiate you before you board a plane. (Some people might call that a "national health plan.") So, here is a gift for Bruce – TSA approved travel locks. Giving a broken lock to one of the world's leading cryptographers will probably not turn out well. For the TSA, I mean.

We read yesterday that the National Security Agency is now collecting photo images. The EPIC staff wants you to be well prepared. So everyone at the dinner tonight gets EPIC approved facial recognition blockers (non-techies call these "sunglasses"). We also have for you RFID envelopes to protect your credit cards and identity documents. (Techies and Supreme Court advocates call these "Faraday bags"). And we have a bracelet that will cover both the camera and the audio port on your cellphone.

This is a special event for EPIC. We are recognizing Champions of Freedom who have helped safeguard privacy and we are recognizing 20 years of EPIC work

A BRIEF HISTORY OF EPIC

EPIC began 20 years ago with the first Internet petition. A group of experts in law and technology objected to the NSA's proposal to monitor the private communications of Internet users. We opposed the "Clipper Chip" with a letter to the President and then a petition signed by 50,000 Internet users. (Glad we solved that problem.)

Our first grant came from the Fund for Constitutional Government, a private foundation established after Watergate to monitor government abuse (thank you, Conrad, and our friends at GAP and POGO)

Our first chairman was John Anderson, the independent candidate for President and a respected Constitutional scholar. We believed it was very important to make clear EPIC's belief that privacy was non-partisan.

David Sobel obtained our first attorney's fees in Freedom of Information Act cases we had litigated against the Department of Justice. (Thank you DOJ for the "seed" funding.)

And Dave Banisar figured out how to attach a 1200 baud modem to a Mac SE. When web software became available we quickly produced one of the ugliest web pages on the Internet. (Some would say we've maintained that tradition.) But it was also very effective and for 20 years, epic.org has remained one of the most authoritative sites on privacy issues in the world.

Key to EPIC's work at the beginning was the expertise of the legal scholars and technical experts who worked with us on the Clipper petition. We quickly formed an Advisory Board of leading experts. Bruce was one of our key experts. In fact, he and Dave Banisar published "The Electronic Privacy Papers" based on many of the documents EPIC obtained under the FOIA.

Over the years our program expanded. We pursued new cases, testified in Congress, filed amicus briefs, petitioned federal agencies, organized campaigns, built coalitions, drafted declarations, published books, articles, and reports. Occasionally, we got our name in the newspaper.

But it was our initial campaign to stop the NSA -- to work with leading experts, to protect privacy, to build public support, to have a real impact -- that shaped our organization and took us to this point.

RECENT ACCOMPLISHMENTS

A year ago we gave awards to Senator Paul and Wyden. Two days later The Guardian broke the story about the "Verizon order," the order from the

Foreign Intelligence Surveillance Court that authorized the bulk collection of all telephone records of American telephone customers.

I thought it was the answer from an old privacy law exam – “draft an unlawful court order.” I took out my pen and started circling. “Relevance to an ongoing investigation” Obviously not. This was easy test. But then I realized this was a real court order. The NSA actually did obtain all that data.

We explored our legal options. Within a few weeks, EPIC filed a petition at the US Supreme Court, supported by legal scholars and former members of the Church Committee. The Court -- after the government sought two extensions which gave the surveillance court just enough time to author and then release an opinion justifying the program – dismissed our petition. But we were right and everyone knew it.

Earlier this year, the President announced significant changes to 215 program. Now there will be a judicial determination prior to a search.

Congress is also moving forward with legislation to reform surveillance in the United States. The USA Freedom Act, sponsored by Senator Leahy and Rep. Sensenbrenner, is the antidote to a decade of false patriotism,

And around the world, many countries are working to update their privacy laws. To the credit of the Europeans, this is not just about the activities of the NSA. There has also been substantial review of the intelligence agencies operating in Europe, as there should be.

We are going to thank someone tonight whose courage helped make this all possible.

Of course, EPIC’s work continues across many domains. We won a significant FOIA case concerning the government’s policy of shutting down telephone service during a peaceful protest. We cannot object to governments in the Middle East that shut down the Internet if our own government maintains a secret policy that stops a public protest here.

The Federal Trade Commission brought an enforcement action against Snapchat after EPIC explained that the delete feature did not delete. We want

companies to develop privacy enhancing techniques, but we also want them to work.

The FTC also warned WhatsApp and Facebook to respect privacy commitments to users after EPIC warned the FTC about the consequences of the proposed acquisition. There are 340m users of WhatsApp, including most of your kids. They and you should know that EPIC is looking out for you.

EPIC also stood up for students and focused public attention on the over-collection of sensitive information on young children. We proposed a Student Privacy Bill of Rights that has provided the basis for legislative efforts in Washington and across the country.

EPIC submitted comments to the White House on the Big Data report. Many of our recommendations were incorporated in the final report, and we were proud of that. But when the President's science advisors failed to acknowledge the risks of big data, we also spoke out.

EPIC continues to play a prominent role in cases that raise novel privacy and civil liberties issues. We filed a substantial amicus brief in *Riley*, the cell phone privacy case currently before the Supreme Court. Both the Court and the Advocates acknowledged the EPIC brief during the oral argument last month.

As with all of our work, this is only possible because of the support we received from friends and colleagues, experts, and supporters. You have helped make a small but dedicated organization effective far beyond its size.

LOOKING AHEAD

It's tempting when a milestone approaches to look backward, recount the many campaigns, and share old stories, but that is not EPIC's orientation. Our focus is always ahead. And our work has never been more urgent

Security breaches and identity theft are on the rise. CNN reported that over half of Americans accounts have been hacked this year and we haven't end made it to the end of June.

But the problems are actually far worse. Your passwords have been compromised. The basic protocols of the Internet are not secure. And yet the President's Scientific and Technical Advisors recommend that companies and agencies continue to gather our personal data.

Washington has been unable to make any substantial progress. The folks at Fort Meade and those at Mountain View both exercise veto power over meaningful privacy reform that would protect American consumers.

EPIC is not waiting for others to act. We never have.

With the support of the MacArthur Foundation, we have undertaken a new project – “EPIC 20/20” – to develop a vision of privacy in the modern age. It is our goal to identify the most pressing challenges and to propose new solutions.

The EPIC Advisory Board met earlier today to discuss our plan.

We begin with the release of a new survey identifying challenges and strategies over the next 20 years. Here are a few preliminary findings from the EPIC Advisory Board:

- In the year 2034, 78% said facial recognition will be routine, but less than half said concealing identity will be a crime
- Physical surveillance is likely to increase substantially
- 57% said it will still be possible to access the Internet anonymously, though 78% said there would be less freedom
- EPIC Advisory Board members, wisely I think favors law and technology over market forces and ethical guidelines
- Overall our Advisory Board is slightly more optimistic than pessimistic, but it's close.

We plan to engage the public as we always have and we plan to propose solutions for the problems we uncover. Tomorrow our survey is open to all.

CLOSING COMMENTS

Finally, I know there was some controversy about this evening's event.

But to be clear, there was an unprecedented discussion that took place among the members of the EPIC Advisory Board about tonight's awardees. There was a wide range of opinions to be sure.

And not everyone agreed about the outcome. But the insight, thought, and conviction that went into our decision made me very proud to be apart of this organization, and also very grateful to have the opportunity to work with such an extraordinary group of people.

EPIC's mission was always to focus public attention on emerging privacy and civil liberties issues. That has not changed and it will not change. I believe it is one of the most important challenges for those living in our age to pursue.

And we have always done what we believed was right and necessary.

Thank you for making it possible for an organization such as EPIC to celebrate 20 years.

We could not have done this without you.